What is claimed is:

1. A processor comprising:

a mechanism to identify memory as secure memory accessible by secure processes, and to identify non-secure memory accessible by both secure and non-secure processes; and

a security enforcement mechanism to allow page tables for the non-secure processes to be stored in secure memory.

2. The processor of claim 1 wherein the processor can operate in a secure mode and in a non-secure mode; and the security enforcement mechanism allows page table walks for non-secure processes while in non-secure mode.

3. The processor of claim 1 wherein the security enforcement mechanism includes page table walk hardware capable of walking page tables in secure memory in response to architecture events caused by non-secure processes.

4. The processor of claim 1 wherein the security enforcement mechanism includes circuits to differentiate between program generated memory accesses and architecture generated memory accesses, and to block program generated memory access from accessing secure memory.

5. The processor of claim 1 further comprising a configurable memory management unit capable of requiring non-secure process to access secure memory when performing page table walks.

6. The processor of claim 1 further comprising virtual address translation hardware to perform virtual address translation for non-secure processes via page tables in secure memory.

7. The processor of claim 1 further comprising a translation look-aside buffer (TLB), wherein the security enforcement mechanism allows a secure memory access after a TLB miss.

8. The processor of claim 1 further comprising a control register to specify whether page tables for non-secure processes are kept in secure memory or non-secure memory.

9. The processor of claim 1 further comprising page table walk hardware capable of accessing secure memory on behalf of non-secure processes.

10. A processor comprising an apparatus to differentiate between hardware generated memory accesses and software generated memory accesses and to grant secure memory access to hardware generated memory accesses.

11. The processor of claim 10 wherein the hardware generated memory accesses are the result of a translation look-aside buffer (TLB) miss.

12. The processor of claim 11 wherein hardware generated memory accesses may be caused by secure or non-secure processes.

13. The processor of claim 10 wherein the hardware generated memory accesses are the result of architecture events.

14. The processor of claim 13 wherein the architecture events result in a page table walk for a non-secure process.

15. A processor comprising circuitry to differentiate between non-secure process having page tables in non-secure memory, secure processes capable of having page

tables in non-secure memory or secure memory, and safer secure processes having page tables in secure memory.

16. The processor of claim 15 wherein the circuitry comprises a memory management unit.

17. The processor of claim 16 wherein the memory management unit comprises a control register to prevent the processor from using non-secure memory when performing a page table walk for a secure process.

18. The processor of claim 15 further comprising page table walk hardware to perform page table walks.

19. The processor of claim 18 wherein the processor can operate in a secure mode or non-secure mode, and the page table walk hardware can perform page table walks without changing the mode in which the processor operates.

20. A method comprising:

determining if a translation look-aside buffer (TLB) miss has occurred;

determining if a current process page table is in secure or non-secure memory; and

if the current process page table is in secure memory, performing a page table walk in secure memory.

21. The method of claim 20 wherein the page table walk is performed for a secure process.

22. The method of claim 20 wherein the page table walk is performed for a non-secure process.

23. The method of claim 20 further comprising if the current process page table is in non-secure memory, performing the page table walk in non-secure memory.

24. An electronic system comprising:

a plurality of antennas;

an amplifier coupled to at least one of the plurality of antennas to amplify communications signals;

a processor coupled to the amplifier; and

memory that can be partitioned by the processor into secure memory accessible by secure processes and non-secure memory accessible by secure or non-secure processes;

wherein the processor includes a security enforcement mechanism to allow page tables for non-secure processes to be stored in secure memory.

25. The electronic system of claim 24 wherein:

the processor can operate in a secure mode and in a non-secure mode; and

the security enforcement mechanism allows page table walks for non-secure processes while in non-secure mode.

26. The electronic system of claim 24 wherein the security enforcement mechanism includes page table walk hardware capable of walking page tables in secure memory in response architecture events caused by non-secure processes.